UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,953	11/30/2000	Guy McIlroy	PALM-3281.US.P	5875

49637 7590 10/07/2011

BERRY & ASSOCIATES P.C.
9229 SUNSET BOULEVARD
SUITE 630
LOS ANGELES, CA 90069

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2494	

NOTIFICATION DATE	DELIVERY MODE
10/07/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

efiling@berrypc.com

Office Action Summary	Application No.	Applicant(s)	
	09/727,953	MCILROY, GUY	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2494	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1 and 4-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1, 4-21* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *17 May 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/2/2011 has been entered.

Response to Amendment

Claims 2-3 and 22-28 have been cancelled. Applicant's arguments/amendments with respect to the pending claims filed 8/2/2011have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

First Action Final Following a Request for Continued Examination

All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the application prior to entry under 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action after the filing of a request for continued examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

Applicants contend that "the discussion of testing is inconsistent with the broadest reasonable construction consistent with the specification." Examiner respectfully disagrees. Examiner has reviewed Applicant's specification which merely indicates that a validator program within the open platform system provides validation of a program before loading it onto the portable device from a host computer or a trusted source on the Internet. Furthermore, the Examiner would like to note that the claim includes open language in regards to the open platform system. Specifically, Applicants use the terminology "comprising" in reference to the open platform system is open language and therefore can comprise more than just a host and portable device. Claim 1 recites "open platform computer system, **comprising** the host facility and the portable computing device." In the system disclosed in Wentker et al., the open platform architecture includes various elements including a terminal connected to a smart card, where the smart card may be included in a personal data assistant (PDA), and additionally includes a card

manager and an issuer/trusted third party which performs testing of the software before the software may be loaded onto the smart card (col. 4, lines 29-40 and lines 57-60). Nowhere does claim 1 limit the claim to an open platform computer system which only contains a portable device and a host facility. Therefore, since the claims incorporate open language, the open platform architecture of Wentker et al. reads on the claim language. If Applicants intend to claim that the validator program is executed by the host facility within the open platform system, as described in various embodiments of Applicant's specification, then Applicants are invited to incorporate that language into the claims so that the claim is interpreted as such. Without any amendments, Examiner believes that the claim limitation "validating the software by the use of a **validator program residing in the open platform computer system**..." only requires a program which performs validation residing within the open platform computer system which **comprises** a host facility and portable device.

Applicants state "Wentker's system is closed because it discloses taking ownership of security domain, the use of secret keys, and assigning secret keys to a provider. If a developer does not belong to this system, their application does not make it to a smart card. Wentker has the benefit of always being able to rely on an application provider being a trusted third party." Applicants further contend "an open platform computer system has the meaning that a vendor or distributor or similar entity does not retain security control of the security features of the computer system." Examiner would first like to point out that the deduction that Wentker's system is closed based on the fact that Wentker discusses the use of security domains for providers is not supported by the explicit teachings of Wentker et al. Wentker et al. explicitly

teach that their invention is geared towards an open platform system in col. 4, lines 29-36 (as well as various other portions):

> In one particular embodiment, the present invention works well with the 'Open Platform' architecture as defined in Open Platform Card Specification Version 2.0, Apr. 19, 1999, available from Visa International Service Association. This architecture is based upon the JAVA Card operating system and provides hardware-neutral, vendor-neutral, application independent card management standard.

Wentker et al. teach the invention in the realm of an open platform architecture in various other portions including but not limited to Fig. 1; Fig. 2; col. 6, lines 1-12 & lines 31-46; col. 7, lines 57-62; col. 8, lines 17-39; and col. 12, lines 1-21. Therefore, Examiner believes it is an improper assessment to suggest that the invention of Wentker et al. is directed to a "closed" system. Furthermore, regarding Applicant's argument directed to the meaning of the term "open platform system," Examiner was unable to locate this particular definition in Applicant's specification. Since this definition does not appear in the specification and Wentker et al. disclose an open platform architecture, the open platform architecture disclosed by Wentker et al. is equivalent to the open platform system of the present invention. Finally, since Applicants disclosure fails to define the term "open platform system" as argued by Applicants, Examiner contends that the provided meaning is not being dismissed and that the meaning may be construed to include other nodes connected within the open platform system lacking a specific definition to the contrary. Examiner invites Applicants to either amend the claim to specify which particular element within the open platform system performs the validation or to point out a specific definition provided in the Applicant's disclosure which is contrary to the Examiner's interpretation applied to the claimed language. Again, Examiner would like to note that the claims have been interpreted broadly, but reasonably according to MPEP 2111. Various embodiments have been disclosed in

Applicant's Specification and it would be improper for the Examiner to incorporate limitations from a particular embodiment of Applicant's specification into the claimed language.

Applicants further contend "Synchronization as used within the specification and the claims means the well-known synchronization process that occurs between a host facility and a portable computing device" and further state that "the present invention must be construed under the context of a synchronization process between an open platform computer system comprises a host facility and a portable computing device." Examiner would like to reiterate that claim 1 calls for an "open platform computer system, **comprising** the host facility and the portable computing device." Nowhere does claim 1 limit the claim to an open platform computer system which only contains a portable device and a host facility. Therefore, since the claims incorporate open language, the open platform architecture of Wentker et al. reads on the claim language. Furthermore, with regards to the term "synchronization," par. 8 of Applicant's PGPUB refers to synchronization as a simple loading step/data exchange between a portable device and a host. Wentker et al. teach an open platform architecture which includes a card terminal and smart card, as well as other elements within the open platform system, where the applications are loaded onto the smart card from some type of card terminal (col. 4, lines 57-60; col. 6, lines 13-30; and Fig. 1). Although the exact term "synchronization" may not be utilized in Wentker et al., the teachings of Wentker et al. are equivalent to the term "synchronization" as described by Applicants PGPUB in par. 8 as mentioned above.

Applicants also contend "An application provider testing software is not equivalent to a pre-synchronization scan" which Applicants define to be "a scan that occurs before the synchronization process yet after the software has been loaded on the platform system

comprising a host facility that directly will be synchronizing with the portable computing device." Examiner would like to note that par. 39-40 Applicant's PGPUB disclose two different embodiments which contain the validator program, one which is the host computer (par. 39 of Applicant's PGPUB) and the other is a secure location on the Internet (par. 40 of Applicant's PGPUB). Based on these two different embodiments, it is clear that even Applicants intended for the validator program to be possibly loaded into the portable device from a host or from a secure location on the Internet where both of these embodiments are within the open platform system. Therefore, the Examiner's interpretation of the term "pre-synchronization" as a phase occurring before loading the application onto the card is supported by the broadest reasonable interpretation in light of the specification.

Applicants further contend "the Examiner appears to skip over the existence of a validator program existing on the open platform system" and assert "the Examiner cannot point to a validation program running within the system." Examiner respectfully disagrees. Wentker et al. teach that an issuer or trusted third party, prior to loading the software onto a smart card, may perform a scan on the application to ensure that the application has no viruses and would pose no threats to the smart card (col. 15, lines 1-19). Once the trusted third party/issuer ensures the smart card does not pose a threat and is ready to be loaded onto the smart card, the software is certified and a data authentication pattern (DAP) which may be digitally signed by the issuer/trusted third party are appended to the software as a validation flag (col. 15, lines 20-67). The validation step occurs at a trusted third party which is a part of the whole open platform system (Fig. 7A, "Delegated Loading" step, element 322, element 326, and element 330 which show that the scanning step occurs before the application is loaded onto the smart card). Also,

Examiner would like to make reference to par. 32 of Applicant's PGPUB which mentions that the validation flag may be a digital signature, where Wentker et al. teach appending a hash of the application which is digitally signed by the trusted third party/issuer for further validation (col. 15, lines 20-67). Furthermore, Examiner would like to note that just because the Wentker et al. reference does not specifically use the terminology "validator program" it does not mean that the concept is not disclosed. One of ordinary skill in the art would interpret a validator program as performing some type of validation/verification of a program/software/application (these terms have equivalent meanings in the art). Therefore, since Wentker et al. teach a program which certifies the application based on performing various checks (col. 15, lines 1-19), Wentker et al. teach a validator program.

Applicants contend that "neither citation references a pre-synchronization scan, a validator program, an emulator, or scanning software by the validator program in a secure environment." Applicants also contend "Wentker contains no concept of a pre-synchronization scan…" and that the cited "passage does not state that the software is marked with a flag during any validation process that would possible deny the software the ability to run on the system and deny synchronization." Examiner respectfully disagrees. Again, a synchronization phase, as described in par. 8 of Applicant's PGPUB, is merely a data exchange/software being loaded onto a portable device. Therefore, pre-synchronization (as used in the scope of the claim) would be any phase before the synchronization/loading phase occurs. Also, once again, Applicants only specify that the software is loaded on the open platform system and does not specify which element of the open platform system comprising of a host facility and portable computing device (as well as possible other nodes within the system such as a secure location on the Internet as

disclosed in the embodiment mentioned in par. 40 of Applicant's PGPUB) actually loads the software in a manner that initiates a pre-synchronization scan. Wentker et al. teach, prior to loading the software to a smart card from a host device, a pre-synchronization scan to ensure that the application approved by the card issuer is identical to that received by the card manager (col. 12, lines 49-57). Furthermore, Wentker et al. teach several other portions where scans occur prior to the phase where the software is eventually loaded onto the host device and eventually onto the portable device (col. 15, lines 6-15). Specifically, Wentker et al. teach that the software may be checked for viruses and other threats (col. 15, lines 14-15). It is clear from the previous citation that Wentker et al. teach utilization of some type of validation program running within the system (again, within any element of the open platform system since the claims fail to specify) in order to check for potentially harmful behavior within each application. Wentker et al. teach that based on the result of the pre-synchronization scan and running the validator program, the application may be marked as being "certified" if it behaves properly and is thus cleared to be loaded (col. 15, lines 15-19), i.e. marking the software as valid (where it is obvious/well-known that it would contrarily be considered invalid and not cleared for loading if it is not marked as "certified"). Furthermore, Examiner would like to note that the claims call for the validator program marking the software as "valid" *or* "invalid," thus the claim only requires that the software is marked as either valid or invalid, where in the previous citation Wentker et al. teach adding a "certified" flag in addition to a data authentication pattern to software marked as valid for yet another verification/validation step of the software before the loading occurs to ensure the integrity of the code is still in tact (col. 15, lines 15-51). Wentker et al. also teach a card-locking feature in col. 9, lines 34-65 plays a role in all of this since it explicitly states that

the "card manager 104 can take control of the application life cycle if the card or the issuer detects a security problem or if the application is to be deleted" (col. 9, lines 63-65). The previous portion of Wentker et al. suggests that the software may automatically be denied the ability to operate/be synchronized within the open platform system if a security problem has been detected and the application fails to operate in a secure manner.

Applicants assert that the issuer/trusted third party disclosed in Wentker et al. is not a part of the open platform system, however Examiner was unable to location a portion of Wentker et al. that specifies the issuer/trusted third party does not fall within the open system architecture disclosed. On the contrary, Wentker et al. teach that the purpose of the open system architecture is to securely load applications independent of various providers onto one smart card (col. 6, lines 31-67). Examiner would also like to direct Applicant's attention to Fig. 1, Fig. 2, Fig. 7A-7B which clearly suggest that the application provider and the issuer are a part of the open platform architecture disclosed in Wentker et al. Any element which is in communication with the open platform architecture may be considered to be a part of that overall system, especially when keeping in mind the manner in which Wentker et al. describe their invention. Therefore, the step of the validator program is performed by an element within the open platform architecture, namely the issuer/trusted third party (col. 15, lines 20-51 and Fig. 7B, element 322). Examiner especially believes this interpretation is reasonable based on one of the possible embodiments disclosed in par. 40 of Applicant's PGPUB which indicates that a secure location on the Internet may be the location at which the validator program resides. Examiner would like to note that given the embodiments disclosed in the specification and the manner in which the invention has been claimed, the Examiner is not limited from interpreting the pre-

synchronization phase as the application testing phase since it occurs before synchronization within the open platform architecture at a trusted third party.

Applicants further contend that Muttik's combination is improper due to impermissible hindsight. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicants further contend that "the suggested combination of Wentker with Muttik is improper" and that "Wentker provides absolutely no motivation, teaching, or suggestion for one ordinarily skilled in the art to consult Muttik (or any reference discussing emulator's for that matter)." Examiner respectfully disagrees. Wentker et al. teach a pre-synchronization phase which implements a validator program in order to determine if a particular application contains viruses or other security threats (col. 15, lines 6-15). Muttik et al. was introduced since Wentker et al. failed to explicitly disclose wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4,

lines 4-23). One of ordinary skill in the art would have been motivated to run the application (which is potentially harmful) in an emulator in a modified operating system since Muttik et al. suggest (and it was well known in the art at the time the invention was made) that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23. Furthermore, in response to Applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, Muttik et al. specifically state "Emulator buffer 201 and emulator code 203 are designed so that while suspect code 108 that is executing within emulator buffer 201, s**uspect code 108 cannot damage or compromise computer system** 106" (col. 4, lines 18-22).

Finally, Applicants contend that "Muttik's scope does not include and thus does not disclose 'a computer system comprising a host facility and a portable computer device coupled to the host facility' (emphasis added)." Examiner would like to point out that Muttik was not relied upon for this feature. Wentker et al. teach the open platform computer system comprising the host facility and the portable computing device (col. 4, lines 43-63 and col. 12, lines 9-21). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on

combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the combination of Wentker et al. and Muttik et al. teach/suggest the claimed invention, including the limitation that states the open platform computer system comprises a host facility and portable computing device. Although Applicants contend that "it is irrelevant that Muttik was not relied upon to teach this functionality," Examiner respectfully disagrees. It is commonly known in the art to run potentially malicious code in an emulator so that if the code is actually harmful the computer system (or portable device in this case) is prevented from being infected/damaged. The Examiner introduced Muttik to support this statement and Muttik provided motivation explicitly stating this notion in the portions cited to above.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 4-5, 8-13, 15-18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and further in view of Muttik et al., US Patent No. 6,907,396.

As per claim 1:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising loading software suitable for operating on an open platform computer system in a secure environment on the open platform computer system comprising the host facility and the portable computing device (col. 4, lines 43-63 and col. 12, lines 9-21); upon loading the software on the open platform computer system, initiating a pre-synchronization scan (col. 12, lines 49-57); during a pre-synchronization scan, validating the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computer device if the validator fails to identify the software as valid in order to ensure the security of the open platform computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the

code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 4:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Furthermore, Wentker et al. teach wherein said software is supplied by a third-party source (col. 13, lines 40-60).

As per claim 5:

Wentker et al. and Muttik et al. substantially teach the method described in claim 4. Furthermore, Wentker et al. teach wherein said third-party software is for execution or other use on a palmtop computer (col. 4, lines 43-63).

As per claim 8:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising a validations program residing on the open platform computer system in a secure fashion that is configured for: a portable computing device coupled to a host computer, wherein the portable computing device is configured to load software from the host computer to the portable computing device for operating on the portable computing device (col.

12, lines 9-21); a validation program residing on the open platform computer system in a secure fashion (col. 12, lines 49-57) that is configured for: validating the software during a pre-synchronization scan by first scanning the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computing device if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 9:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Muttik et al. teach wherein said host computer is coupled to a network (col. 3, lines 54-62).

As per claim 10:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a handheld computing device (col. 4, lines 43-63).

As per claim 11:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 12:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an infrared device (col. 5, lines 28-40).

As per claim 13:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an RF enabled device (col. 5, lines 28-40).

As per claim 15:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Wentker et al. further teach wherein said validation program is configured to evaluate third-party

software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12, line 58 – col. 13, line 10 and col. 15, lines 1-19).

As per claim 16:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 15. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-51).

As per claim 17:

Wentker et al. and Muttik et al. substantially teach the apparatus described claim 15. Furthermore, Wentker et al. teach wherein said portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 18:

Wentker et al. substantially teach an apparatus of ensuring the security of an open platform computer system, comprising a validations program residing on the network that is configured for: a handheld computing device coupled to a network, wherein the handheld computing device is configured to load software from the network to the handheld computing device for operation on the handheld computing device (col. 4, lines 43-63 and col. 12, lines 9-21); validating the software by scanning files of the software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld

computing device (col. 12, lines 49-57); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 20:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-

51).

As per claim 21:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12, line 58 – col. 13, line 10 and col. 15, lines 1-19)

III. Claims 6, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claims 1, 8, & 18 above, and further in view of Ginter et al., US Patent No. 6,948,070.

As per claim 6:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Not explicitly disclosed is wherein said validator program is specially constructed to reside in a secure fashion in the host facility of said computer system. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so

since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 14:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Not explicitly disclosed is wherein said validation program resides in said host computer of the computer system in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 19:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Not explicitly disclosed is wherein said validation program resides in said computer network in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for

the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

IV. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claim 1 above, and further in view of Brody, US Pub. No. 2001/0051928.

As per claim 7:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Muttik et al. also teach a host computer (col. 3, lines 54-62). Furthermore, Muttik et al. teach that the computing environment allows for various computing systems, one of which may be a personal organizer (col. 3, lines 44-49). Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer and wherein the validating operation is performed by the host computer for the portable computing device. However, Brody teaches a PDA coupled to a host device for personalization purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the palmtop computing device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so

since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA in par. 33, lines 1-30.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,694,436
2. US Patent No. 5,953,502
3. US Patent No. 7,080,407
4. US Patent No. 6,981,279
5. US Patent No. 6,481,632 – cited in reference to an "open platform" architecture/system
6. US Patent No. 7,243,236
7. US Pub. No. 2002/0069263
8. US Patent No. 6,662,020 – found in update search performed 9/27/2011, seems relevant

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Kim can be reached at (571) 272-3804. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2494
9/28/2011

NK

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431